Structured optical receivers to attain superadditive capacity and the Holevo limit

Saikat Guha

Disruptive Information Processing Technologies group,
Raytheon BBN Technologies, Cambridge, MA 02138, USA

When classical information is sent over a quantum channel, attaining the ultimate limit to channel capacity requires the receiver to make joint measurements over long codeword blocks. For a pure-state channel, we construct a receiver that can attain the ultimate capacity by applying a single-shot unitary transformation on the received quantum codeword followed by simultaneous (but separable) projective measurements on the single-modulation-symbol state spaces. We study the ultimate limits of photon-information-efficient communications on a lossy bosonic channel. Based on our general results for the pure-state quantum channel, we show some of the first concrete examples of codes and structured joint-detection optical receivers that can achieve fundamentally higher (superadditive) channel capacity than conventional receivers that detect each modulation symbol individually.

When the modulation alphabet of a communication channel are quantum states, the Holevo limit is an upper bound to the Shannon capacity of the physical channel paired with any receiver measurement. Even though the Holevo limit is an achievable capacity, the receiver in general must make joint (*collective*) measurements over long codeword blocks—measurements that can't be realized by detecting single modulation symbols followed by classical post processing. This phenomenon of a joint-detection receiver (JDR) being able to yield higher capacity than any single-symbol receiver measurement, is often termed as *superadditivity* of capacity.

For the lossy bosonic channel, a coherent-state modulation suffices to attain the Holevo capacity, i.e., non-classical transmitted states do not yield any additional capacity [1]. Hausladen et. al.'s square-root-measurement (SRM) [2], which in general is a positive operator-valued measure (POVM), applied to a random code gives us the mathematical construct of a receiver that can achieve the Holevo limit. Lloyd et. al. [3] recently showed a receiver that can attain the Holevo capacity of any quantum channel by making a sequence of "yes/no" projective measurements on a random codebook. Sasaki et. al. [4], in a series of papers, showed several examples of superadditive capacity using pure-state alphabets and the SRM. However, the key practical questions that remain unanswered are how to design modulation formats, channel codes, and most importantly, structured realizations of Holevo-capacity-approaching JDRs.

In this paper, (i) we show that the Holevo limit of a pure-state channel is attained by a projective measurement, which can be implemented by a unitary operation on the quantum codeword followed by separable projective measurements on the single-modulation-symbol subspaces, (ii) we translate our result into an optimal receiver for the lossy bosonic channel, and (iii) we show concrete examples of codes and receivers that yield superadditive capacity for optical binary-phase-shift keying (BPSK) signaling at low photon numbers. These, we believe, are the first receiver realizations that can exhibit superadditivity, and can be tested using laboratory optics.

Attaining Holevo limit of a pure-state channel. We encode classical information using a Q-ary modulation alphabet of non-orthogonal pure-state *symbols* in $S \equiv \{|\psi_1\rangle, \ldots, |\psi_Q\rangle\}$. Each *channel use* constitutes sending one symbol. We assume that the channel preserves the purity of S, thus taking the states $\{|\psi_q\rangle\}$ to be those at the receiver. The only source of noise is the physical detection of the states. Assume that the receiver detects each symbol one at a time. Channel capacity is given by the maximum of the single-symbol mutual information,

$$C_1 = \max_{\{p_i\}} \max_{\left\{\hat{\Pi}_j^{(1)}\right\}} I_1\left(\{p_i\}, \left\{\hat{\Pi}_j^{(1)}\right\}\right) \text{ bits/symbol}, \quad (1)$$

where the maximum is taken over priors $\{p_i\}$ over the alphabet and a set of POVM operators $\left\{\hat{\Pi}_j^{(1)}\right\}$, $1 \leq j \leq J$ on the single-symbol state-space. The measurement of each symbol produces one of J possible outcomes, with conditional probability $P(j|i) = \langle\psi_i|\hat{\Pi}_j^{(1)}|\psi_i\rangle$. To achieve reliable communications at a rate close to C_1, forward error-correction will need to be applied on the discrete memoryless channel with transition probabilities $P(j|i)$. In other words, for any rate $R < C_1$, there exists a sequence of codebooks $\mathcal{C}_n$ with $K = 2^{nR}$ codewords $|\boldsymbol{c}_k\rangle$, $1 \leq k \leq K$, each codeword being an n-symbol tensor product of states in S, and a decoding rule, such that the average probability of decoding error (guessing the wrong codeword), $\bar{P}_e^{(n)} = 1 - \frac{1}{K}\sum_{k=1}^{K} \Pr(\hat{k} = k) \to 0$, as $n \to \infty$. In this 'Shannon' setting, optimal decoding is a maximum likelihood (ML) decision, which can in principle be pre-computed as a table lookup (see Fig. 1). We define C_n as the maximum capacity achievable with measurements that jointly detect up to n symbols. The fact that joint detection allows for $C_{n+m} > C_n + C_m$, (or $C_n > C_1$) is referred to as *superadditivity* of capacity. The Holevo-Schumacher-Westmorland (HSW) theorem says,

$$C_\infty \equiv \max_{\{p_i\}} S\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) = \lim_{n\to\infty} C_n, \quad (2)$$

the Holevo bound, is the ultimate capacity limit, where $S(\hat{\rho}) = -\text{Tr}\hat{\rho}\log_2\hat{\rho}$ is the von Neumann entropy, and

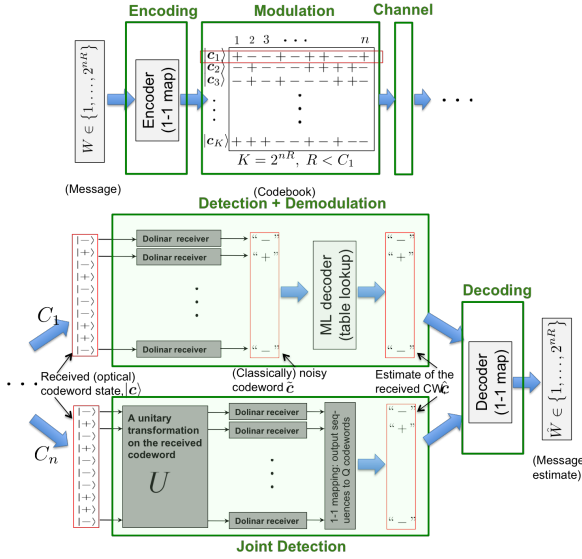FIG. 1: Classical communication system, shown here for a BPSK alphabet. If the receiver uses symbol-by-symbol detection, maximum capacity = C_1 bits/symbol. If the Detection+Demodulation block is replaced by a general n-input n-output quantum measurement, maximum capacity = C_n bits/symbol. Superadditivity: $C_\infty > C_n > C_1$, where C_∞ is the Holevo limit. The joint-detection structure shown achieves Holevo limit for BPSK over a lossy bosonic channel.

that C_∞ is achievable with joint detection over long codeword blocks. Calculating C_∞ however, doesn't require the knowledge of the optimal receiver measurement. In other words, if we replaced the detection and demodulation stages in Fig. 1 by one giant quantum measurement, then for any rate $R < C_\infty$, there exists a sequence of codebooks $\mathcal{C}_n$ with $K = 2^{nR}$ codewords $|\boldsymbol{c}_k\rangle$, $1 \leq k \leq K$, and an n-input n-output POVM over the n-symbol state-space $\left\{\hat{\Pi}_k^{(n)}\right\}$, $1 \leq k \leq K$, such that the average probability of decoding error, $\bar{P}_e^{(n)} = 1 - \frac{1}{K}\sum_{k=1}^{K}\langle\boldsymbol{c}_k|\hat{\Pi}_k^{(n)}|\boldsymbol{c}_k\rangle \to 0$, as $n \to \infty$.

Theorem 1: For a pure-state channel, a projective measurement can attain C_∞, and can be implemented as a unitary transformation on the codeword followed by a parallel set of separable single-symbol measurements.

Proof: Consider a codebook $\mathcal{C}$ with $K = 2^{nR}$ codewords $|\boldsymbol{c}_k\rangle$, $1 \leq k \leq K$, each codeword being an n-symbol tensor product of states in S. The SRM (which in general is a POVM) on a random codebook can achieve the Holevo capacity [2]. However, Helstrom showed that the minimum probability of error (MPE) measurement for discriminating K pure states with the least average probability of error is a K-element projective measurement on the span of those K states [7]. By definition, the MPE measurement on $\mathcal{C}$ must achieve a lower average probability of error in discriminating the codewords in $\mathcal{C}$ than the SRM. Hence, the MPE measurement is capacity achieving. In other words, given any *reliable communication*
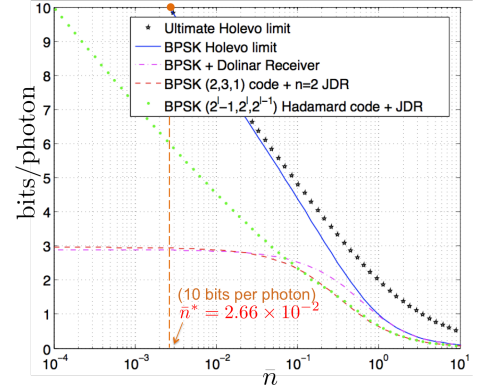

FIG. 2: Photon information efficiency (bits per received photon) as a function of mean photon number per mode, $\bar{n}$.

threshold on the decoding error rate, P_{th}, there exists a codebook $\mathcal{C}$ of a long enough length n, such that the MPE measurement on $\mathcal{C}$ described by the projectors $\left\{\hat{\boldsymbol{\Pi}}_{\text{MPE}}^{(n)}\right\}$ with $\hat{\Pi}_{\text{MPE},k}^{(n)} = |\boldsymbol{w}_k\rangle\langle\boldsymbol{w}_k|$ (where $\{|\boldsymbol{w}_1\rangle, \ldots, |\boldsymbol{w}_K\rangle\}$ form a complete ortho-normal (CON) basis for span($\mathcal{C}$)), can attain a probability of decoding error $P_e^{(n)} = 1 - (1/K)\sum_{k=1}^{K}|\langle\boldsymbol{c}_k|\boldsymbol{w}_k\rangle|^2 \leq P_{\text{th}}$. Now, let us define the MPE measurement on the states in S as $\hat{\Pi}_{\text{MPE}}^{(1)} \equiv \{|m_q\rangle\langle m_q|\}$, where $\{|m_1\rangle, \ldots, |m_Q\rangle\}$ is a CON basis of the single-symbol state space $\mathcal{H}_1 \equiv \text{span}(S)$. Let us define the Kronecker-product CON basis of the n-symbol state space $\mathcal{H}_n = \mathcal{H}_1^{\otimes n}$, $M \equiv \{|\boldsymbol{m}_1\rangle, \ldots, |\boldsymbol{m}_{Q^n}\rangle\}$, where $|\boldsymbol{m}_{\boldsymbol{q}}\rangle = |m_{q_1}\rangle|m_{q_2}\rangle \ldots |m_{q_n}\rangle$, where $q_k \in [1, \ldots, Q]$, $\forall k$. Let us define another CON basis of the n-symbol state space $\mathcal{H}_n$ by extending $\{|\boldsymbol{w}_1\rangle, \ldots, |\boldsymbol{w}_K\rangle\}$—the vectors describing the MPE measurement on $\mathcal{C}$—as $W \equiv \{|\boldsymbol{w}_1\rangle, \ldots, |\boldsymbol{w}_K\rangle, |\boldsymbol{w}_{K+1}\rangle, \ldots, |\boldsymbol{w}_{Q^n}\rangle\}$. Finally, let us extend the codebook $\mathcal{C}$ into the set of *all* Q^n length-n sequences of modulation symbols $\mathcal{C}^E \equiv \{|\boldsymbol{c}_1\rangle, \ldots, |\boldsymbol{c}_K\rangle, |\boldsymbol{c}_{K+1}\rangle, \ldots, |\boldsymbol{c}_{Q^n}\rangle\}$, and express each $|\boldsymbol{c}_k\rangle$ in both CON bases M and W, $|\boldsymbol{c}_k\rangle = \sum_{j=1}^{Q^n}\langle\boldsymbol{m}_j|\boldsymbol{c}_k\rangle|\boldsymbol{m}_j\rangle$, $|\boldsymbol{c}_k\rangle = \sum_{j=1}^{Q^n}\langle\boldsymbol{w}_j|\boldsymbol{c}_k\rangle|\boldsymbol{w}_j\rangle$, where $\langle\boldsymbol{m}_j|\boldsymbol{c}_k\rangle \equiv (U_M)_{kj}$ and $\langle\boldsymbol{w}_j|\boldsymbol{c}_k\rangle \equiv (U_W)_{kj}$ are $(k,j)^{\text{th}}$ elements of the unitary matrices U_M and U_W. The bases M and W are unitarily equivalent. Thus, the MPE measurement on $\mathcal{C}$ is equivalent to first applying a unitary U on the codeword followed by the projective measurement described by M, which is essentially n parallel (and separable) MPE measurements $\left\{\hat{\Pi}_{\text{MPE}}^{(1)}\right\}$, on the single-symbol subspaces. The unitary U is given by (in the basis M),

$$U = \sum_{k=1}^{Q^n}\sum_{j=1}^{Q^n} u_{jk}^* |\boldsymbol{m}_j\rangle\langle\boldsymbol{m}_k|; \quad u_{jk} = \left(U_W^{-1}U_M\right)_{jk}. \quad (3)$$

Superadditive optical receivers. Consider a single-mode lossy bosonic channel (such as a far-field single-spatial-mode free-space-optical (FSO) channel), where data is modulated using a succession of pulses (orthogo-

nal temporal modes) with mean received photon number $\bar{n}$ per mode, where each temporal mode (pulse) carries one modulation symbol. The Holevo capacity is given by, $C_{\mathrm{ult}}(\bar{n}) = g(\bar{n}) = (1 + \bar{n})\log_2(1 + \bar{n}) - \bar{n}\log_2\bar{n}$ bits/symbol, which is attained using a coherent-state modulation, i.e., non-classical modulation states can't get any higher capacity [1]. Since pure loss preserves coherent states (with linear amplitude attenuation), it suffices to define capacity as a function of the mean photon number per *received* mode $\bar{n}$, and the results derived above for a pure-state channel applies. Achieving the Holevo limit requires an optimal codebook and joint measurement on long codeword blocks. At high $\bar{n}$, symbol-by-symbol heterodyne detection asymptotically achieves $C_{\mathrm{ult}}(\bar{n})$. The low photon number ($\bar{n} \ll 1$) regime is more interesting for far-field FSO communications, where the joint-detection gain is most pronounced.

In Fig. 2, we show the photon information efficiency (PIE), the number of bits that can be reliably decoded per received photon, as a function of $\bar{n}$ [12]. There is no fundamental upper bound to the PIE; however, higher PIE necessitates lower $\bar{n}$. Furthermore, binary modulation and coding is sufficient to meet the Holevo limit at low $\bar{n}$. Specifically, the binary-phase-shift keying (BPSK) alphabet $S_1 \equiv \{|\alpha\rangle, |-\alpha\rangle\}$, $|\alpha|^2 = \bar{n}$, is the Holevo-optimal binary modulation at $\bar{n} \ll 1$. Dolinar proposed a structured receiver that realizes the binary MPE projective measurement on an a pair of coherent states using single photon detection and coherent optical feedback [5]. If the Dolinar receiver (DR) is used to detect each symbol, the BPSK channel is reduced to a classical binary symmetric channel (BSC) with capacity $C_1 = 1 - H(q)$ bits/symbol, $q = [1 - \sqrt{1 - e^{-4\bar{n}}}]/2$. This is the maximum achievable capacity when the receiver detects each symbol individually, which includes all conventional (direct-detection and coherent-detection) receivers. The PIE $C_1(\bar{n})/\bar{n}$ caps out at $2/\ln 2 \approx 2.89$ bits/photon at $\bar{n} \ll 1$. Closed-form expressions and scaling behavior of C_n, the maximum capacity achievable with measurements that jointly detect up to n symbols, for $n \geq 2$ are not known. However, the Holevo limit of BPSK, $C_\infty(\bar{n}) = H([1 + e^{-2\bar{n}}]/2)$, can be calculated using Eq. (2). Good codes and JDRs will be needed to bridge the huge gap between the PIEs $C_1(\bar{n})/\bar{n}$ and $C_\infty(\bar{n})/\bar{n}$, shown in Fig. 2. It is interesting to reflect on the point shown by the orange circle (at 10 bits/photon) in Fig. 2, which says that for a 1.55μm far-field FSO system operating at 1 GHz modulation bandwidth, the laws of physics permit reliable communications at 0.266 Gbps with only 3.4 pW of average (and peak) received optical power!

A two-symbol superadditive JDR— Some examples of superadditive codes and joint measurements have been reported [4, 6], but no structured receiver designs. An ensemble (a $(2, 3, 1)$ inner code [13]) containing three of the four 2-symbol BPSK states, $S_2 \equiv \{|\alpha\rangle|\alpha\rangle, |\alpha\rangle|-\alpha\rangle, |-\alpha\rangle|\alpha\rangle\}$, with priors $(1 - 2p, p, p)$,
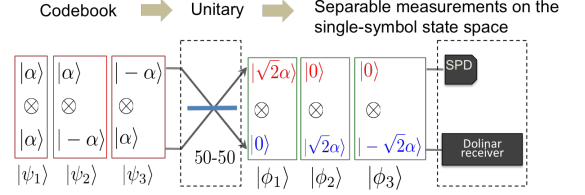

FIG. 3: A two-symbol JDR that attains $\approx 2.5\%$ higher capacity for BPSK than the best single-symbol (Dolinar) receiver.

$0 \leq p \leq 0.5$, can attain, with the best 3-element projective measurement in span(S_2), up to $\approx 2.8\%$ higher capacity that C_1 [6]. Since this is a Shannon capacity result, a classical outer code with codewords comprising of sequences of states from S_2 will be needed to achieve this capacity $I_2 > C_1$. Using the MPE measurement on S_2 (which can be analytically calculated [7], unlike the numerically optimized projections in [6]), $I_2/C_1 \approx 1.0266$ can be obtained. A receiver that involves a unitary operation on the $[2, 3, 1]$ code (a beamsplitter) followed by two separable single-symbol measurements (in this case, a single-photon detector (SPD), and a DR) (see Fig. 3), can attain $I_2/C_1 \approx 1.0249$ (see Fig. 2). Its likely that none of these projective measurements on S_2 attain C_2, since the single-shot measurement that maximizes the accessible information in S_2 could in general be a 6-element POVM [8]. However, *Theorem 1* proves that as the size of the inner code $n \to \infty$, a projective measurement on the codebook that involves an n-mode unitary followed by a DR-array is capable of attaining C_∞, without any additional outer code (see Fig. 1).

An n-symbol superadditive JDR— A $(2^l - 1, 2^l, 2^{l-1})$ BPSK Hadamard code, with $\bar{n}$-mean-photons BPSK symbols, has the same geometry (mutual inner-products) and thus is unitarily equivalent to the $(2^l, 2^l, 2^{l-1})$ pulse-position-modulation (PPM) code with $2^l\bar{n}$-mean-photon PPM pulses. The former is slightly *space-efficient*, since it achieves the same equidistant distance profile, but with one less symbol. Consider a BPSK Hadamard code detected by a 2^l-mode unitary transformation (with one ancilla mode prepared locally at the receiver, in the $|\alpha\rangle$ state) built using $(n\log_2 n)/2$ 50-50 beamsplitters arranged in a fast-fourier-transform (FFT) butterfly circuit, followed by a separable $n = 2^l$-element SPD-array, as shown (for $n = 8$) in Fig. 4(a). The beamsplitter array is reminiscent of the fast Walsh Hadamard transform, if we recall that each 50-50 beamsplitter implements an order-2 FFT. The beamsplitters 'unravel' the BPSK codebook into a PPM codebook, separating out the photon energies in spatially separated bins, making possible discriminating the codewords using a SPD array. This receiver design is a more 'natural' choice for spatial modulation, across, say orthogonal spatial modes of a near-field FSO channel. The ancilla mode at the receiver necessitates a local oscillator phase locked to the received pulses, which is hard to implement. Since the number
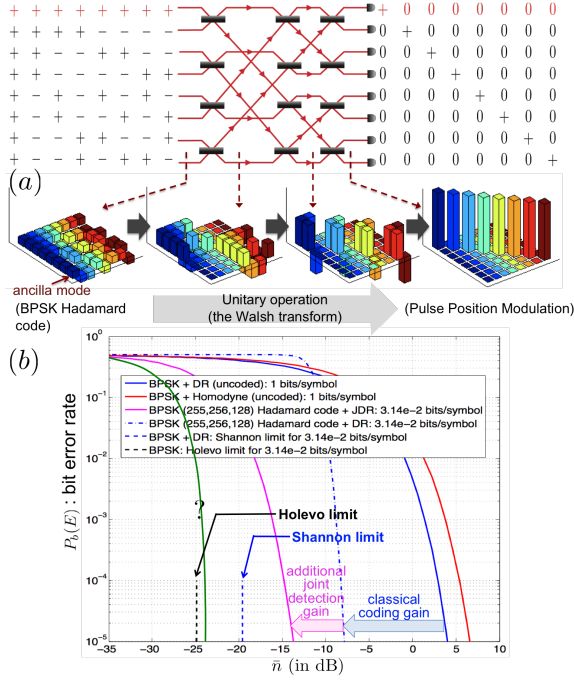
FIG. 4: (a) The BPSK $(7,8,4)$ Hadamard code is unitarily equivalent to the $(8,8,4)$ pulse-position-modulation (PPM) code via a Walsh transform built using twelve 50-50 beam-splitters. (b) Bit error rate plotted as a function of $\bar{n}$.

of ancilla modes doesn't scale with the size of the code, we can append the ancilla mode to the transmitted code-word, so that the received ancilla can serve as a pilot tone for our interferometric receiver. The Shannon capacity of this code-JDR pair—allowing coding over the *erasure outcome* (no clicks registered at any SPD element)—is $I_n(\bar{n}) = (\log_2 K/K)(1 - \exp(-2d\bar{n}))$ bits/symbol. In Fig. 2, we plot the envelope, $\max_n I_n(\bar{n})/\bar{n}$ (the green dotted plot), as a function of $\bar{n}$. This JDR not only attains a *much* higher superadditive gain than the $n = 2$ JDR we describe above, it doesn't need phase tracking and coherent optical feedback like the DR. Note that n-ary PPM signaling also achieves the capacity $I_n(\bar{n})$ with a SPD receiver, albeit with a much higher $(\times 2^l)$ peak power as compared to BPSK. However, *Theorem 1* says that the receiver construct shown in Fig. 1 is capable of bridging the rest of the gap to the Holevo limit (i.e., the blue plot in Fig. 2) in conjunction with an optimal BPSK code. *Theorem 1* applies readily to any higher-order mod-ulation format ($Q > 2$, required to achieve capacity at higher $\bar{n}$), where the DR in the JDR structure must be replaced by an extension of the DR that discriminates Q modulation symbols at their MPE limit (not known yet). Finally, note that in the proof of *Theorem 1*, the MPE measurement on the single-symbol space $\hat{\Pi}^{(1)}_{\mathrm{MPE}}$, was just a convenient choice; any other projective measurement would've worked. In the optimal JDR for BPSK there-fore, the DRs can be replaced by an array of Kennedy re-ceivers (which applies a coherent shift by $-\alpha$ followed by

SPD—a lot simpler than the DR), since it also performs a projective measurement on span(S_1). In Fig. 4(b), we plot the bit error rates $P_b(E)$ as a function of $\bar{n}$ for un-coded BPSK, and the $[255, 256, 128]$ BPSK Hadamard code, when detected using a symbol-by-symbol DR and our structured JDR, respectively. The *coding gain* now has two components, a (classical) coding gain, and an additional *joint-detection gain*.

A great deal is known about binary codes that achieve low bit error rates on the BSC at $\bar{n}$ very close to the Shannon limit [9]. It would be interesting to see how close to the Holevo limit can these same codes perform, when paired with their respective quantum MPE mea-surements. It will be useful to design codes with symme-tries that allow them to approach Holevo capacity, with the unitary U of the JDR in Fig. 1 realizable via a sim-ple network of beamsplitters, phase shifters, two-mode squeezers, and Kerr non-linearities (which form a uni-versal set for realizing an arbitrary multimode bosonic unitary [10]) along with a low-complexity outer code, if at all. The fields of information and coding theory have had a unique history. Even though many of its ultimate limits were determined in Shannon's founding paper [11], it took generations of magnificent coding theory research, to ultimately find practical capacity-approaching codes. Even though realizing reliable communications on an op-tical channel close to the Holevo limit might take a while, it certainly does seem to be in the visible horizon.

[1] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).
[2] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmore-land, W. K. Wootters, Phys. Rev. A **54**, 3 (1996).
[3] S. Lloyd, V. Giovannetti, L. Macconne, arXiv:1012.0106v1 [quant-ph], (2010).
[4] M. Sasaki, K. Kato, M. Izutsu, O. Hirota, Phys. Rev. A **58**, 159 (1998).
[5] S. J. Dolinar, Ph.D. thesis, MIT (1976).
[6] J. R. Buck, S. J. van Enk, C. A. Fuchs, Phys. Rev. A **61**, 032309, (2000).
[7] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic, New York, (1976).
[8] P. Shor, arXiv:0206058v3 [quant-ph], (2003).
[9] G. D. Forney, *Concatenated Codes*, MIT Press, Cam-bridge, MA, (1966).
[10] S. Sefi, P. Loock, arXiv:1010.0326v1 [quant-ph], (2010).
[11] C. E. Shannon, *Bell System Technical Journal* **27**, (1948).
[12] PIE is a more useful metric to communication engineers than channel capacity $C(\bar{n})$. It translates readily into a tradeoff between *photon efficiency*, $C(\bar{n})/\bar{n}$ bits/photon, and *spectral efficiency*, $C(\bar{n})$ bits/sec/Hz.
[13] An (n, K, d) code has K length-n codewords, such that the minimum Hamming distance between any pair of codewords is d. The *code rate* is $R = \log_2 K/n$.